004.057.5+004.056

студент Д.Р. Череватенко, ас. М.В. Торбєєва
ДВНЗ «Національний гірничий університет»

РЕКОМЕНДАЦІЇ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МОБІЛЬНИХ ПРИСТРОЇВ

В даній статті розглянуті деякі проблеми безпеки мобільних пристроїв та надані рекомендації щодо їх запобігання.

В наш час, коли можливості мобільних пристроїв наздоганяють можливості персональних комп'ютерів (ПК), і коли ринок мобільних пристроїв вже обігнав ринок ПК з'являється таке поняття як конс'юмерізація. Конс'юмерізація – використання співробітниками компаній власних мобільних пристроїв для роботи з корпоративною інформацією. Але цей процес також має негативну сторону – безпеку мобільних пристроїв. Обробка важливої інформації на мобільних пристроях призводить до зацікавленості зі сторони зловмисників. Через це виникають такі проблеми як, віруси, перехоплення інформації радіоканалами, крадіжка мобільних пристроїв ті інші проблеми. Тому захист мобільних пристроїв, що обробляють важливу інформацію є на сьогоднішній час актуальним.

Розглянемо декілька порад щодо забезпечення безпеки пристроїв зв'язку.

1. Вибір мобільної операційної системи (ОС), яка підтримує шифрування

Для забезпечення безпеки мобільного пристрою треба використовувати мобільну ОС і пристрій, які підтримують апаратне шифрування для внутрішніх та зовнішніх накопичувачів. Це допомагає захистити дані, навіть від сучасних хакерів. Без шифрування цілком можливо, що хтось зможе обійти пін-код, блокування або пароль і отримати доступ до даних.

2. Встановлення блокування або паролю

Встановлення пароля і пін-кода є першою лінією оборони у захисті секретності і безпеки мобільного пристрою. Це допомагає захиститися від несанкціонованого доступу до нього у разі втрати, крадіжки або в моменти,

коли пристрій залишено без нагляду. Це також необхідно, якщо на пристрої використовується шифрування.

Якщо шифрування не підтримується ОС, все одно треба встановлювати пароль. Хоча деякі зловмисники можуть обійти пароль і отримати доступ до даних, це слугуватиме захистом від звичайного підглядання.

3. Автоочищення даних

Більшість мобільних ОС підтримують автоматичне стирання даних пристрою після певного числа невдалих спроб аутентифікації. Це корисно, якщо шифрування не підтримується пристроєм, але так само корисно і на пристроях, що підтримують шифрування. Необмежена кількість спроб введення пароля призводить до можливості атаки грубою силою, що в кінцевому результаті веде до розсекречування інформації.

Разом з очищенням треба проводити регулярне резервне копіювання і використовувати рішення, які дозволять відновити дані на іншому пристрої.

4. Налаштування віддаленого спостереження і керування

Перш ніж пристрій буде втрачено або вкрадено, треба налаштувати дистанційне відстеження і керування. Це дозволить побачити місце розташування на карті, відправити звукове повідомлення, щоб допомогти знайти пристрій або відобразити візуальні повідомлення. Як правило, вони також дозволяють віддалено заблокувати або знищити пристрій перш, ніж ним заволодіє зловмисник.

5. Обмеження використання точок доступу Wi-Fi

Коли використовується суспільна точка доступу Wi-Fi, яка не використовує шифрування, весь Інтернет-трафік передається повітрям і може бути перехоплений. Найбільш важливі сайти і сервіси, такі як банківські, зазвичай, реалізують своє власне (HTTPS/SSL) шифрування, яке захищає їх індивідуальний трафік. Але більшість постачальників послуг електронної пошти та соціальних мереж шифруванням не користуються. Таким чином, при їх використанні більш вірогідна ймовірність перехоплення паролів і трафіку.

З іншого боку, більшість 3G, 4G, а також інших протоколів стільникового зв'язку, зазвичай шифруються. До того ж ці з’єднання не часто прослуховують. Тому, коли потрібно отримати доступ до даних, використовуйте підключення за допомогою 3G або 4G, а не точки доступу Wi-Fi.

Якщо ж є потреба у використанні точки доступу Wi-Fi, необхідно застосовувати ті точки доступу, які забезпечують шифрування і перевірку автентичності 802.1X. В якості альтернативи можна з’єднуватися за допомогою VPN для забезпечення безпеки трафіку від локальних перехоплювачів.

6. Використання антивірусного програмного забезпечення (ПЗ)

Віруси, шкідливе ПЗ та хакерські атаки на мобільних пристроях ще не дуже розповсюджені, але вони поступово розвиваються. Тому слід розглянути питання про встановлення додатків забезпечення безпеки з метою запобігання заражень і вторгнень. Більшість антивірусів також пропонує додаткові функції, такі як віддалене знищення та резервне копіювання.

Це лише невелика кількість рекомендацій. Але їх використання дозволить підвищити рівень безпеки особистих і важливих даних. Отже, зазначені рекомендації допоможуть не тільки забезпечити безпеку мобільних пристроїв, а й полегшити роботу як співробітникам, так і підприємству в цілому.

Перелік літератури:

1. http://lukatsky.blogspot.com/2011/07/blog-post_05.html
2. http://www.ecohome.ru/life_hardware/?id=649
3. http://www.cioupdate.com/technology-trends/6-tips-for-better-mobile-security.html